

CLAIMS

Sub
GI

1. In an information input device, the combination of:

- a) means for inputting first information;
- b) means for storing secret key information; and
- c) means for generating a digital signature based upon the first information and the secret key information.

2. An information input device according to claim 1, wherein said information is image data.

3. An information input device according to claim 1, wherein the means for generating a digital signature carries out an operation and outputs said digital signature.

4. An information input device according to claim 3, wherein said operation uses public key cryptography.

5. An information input device according to claim 3, wherein said operation for obtaining a digital signature uses RSA cryptosystem.

6. An information input device comprising:

- a) means for inputting first information;
- b) means for compressing said first information;
- c) means for storing secret information; and
- c) means for generating a distinguishing information based on the secret information and the information compressed by said compressing means.

7. An information input device according to claim 6, wherein said information is image data.

A
8. An information input device according to claim 6, wherein said means for generating ~~carries~~ carries out an operation and outputs said distinguishing information.

9. An information input device according to claim 8, wherein said operation is for obtaining a digital signature as said distinguishing information by using a RSA cryptosystem.

~~Subj. 1033~~
10. An image input apparatus comprising:
a) an image input device for inputting said image data;
b) a memory for storing secret information; and
c) an operation device for carrying out an operation using the image data and the secret information.

11. An information input device according to claim 10, wherein said ~~means for generating~~ ~~operation device carries~~ carries out an operation and outputs said distinguishing information.

12. An information input device according to claim 11, wherein said operation is for obtaining a digital signature as said distinguishing information by using a public key cryptosystem.

13. An information input device according to claim 11, wherein said operation is for obtaining a digital signature as said distinguishing information by using a RSA cryptosystem.

00722446 042203

~~Claim 14~~
14. An image input system comprising:

- a) a first terminal device for inputting image data;
- b) a second terminal device for having a memory for storing secret information; and
- c) an operator for executing a command based on an algorithm for generating a digital signature by using the image data and the secret information.

15. An image input system according to claim 14, wherein said algorithm is based on a public key cryptosystem.

16. An image input system according to claim 15, wherein said secret information is a secret key of said public key cryptosystem.

17. An image input system according to claim 14, wherein said algorithm is based on a RSA cryptosystem.

18. An image input system according to claim 14, further having a CODEC for compressing the image data based on a compression algorithm.

19. An image input system according to claim 18, wherein said compression algorithm is based on MPEG standard.

20. An image input system according to claim 18, wherein said compression algorithm is based upon JPEG standard.

21. A device comprising:

- input means to input image data;
- input means to input a distinguishing data corresponding to said image data; and
- verification means for using public key information to verify said image data based on said distinguishing data.

22. A device according to claim 21, wherein said secret information is a secret key of a public key cryptosystem.

23. In an information input device, the combination of:

- means for encrypting information according to a first algorithm; and
- means for encrypting a digital signature according to a second algorithm;

the first algorithm being such that it may be used to encrypt only by said input device; and

the other of said algorithms being such that the data it encrypts can be decrypted only by a designated receiving party.

24. An information input device according to claim 23, wherein said information is image data.

25. An information input device according to claim 23, wherein the means associate with the other algorithm further encrypts data which was encrypted by said one algorithm.

Approved

*Patent
Office*